REMARKS

Claims 1-53 are pending in the present application. Claims 37-43 are herein amended. Applicant believes that the present application is in condition for allowance, which prompt and favorable action is respectfully requested.

I. REJECTIONS UNDER 35 U.S.C. §101

The Office Action rejected claims 37-43 under 35 U.S.C. §101 as being directed to non-statutory subject matter. Specifically, the Office Action notes that independent claim 37 recites "a medium for generating a key stream" which is non-statutory subject matter. Claims 38-43 were rejected as being dependent on claim 37.

Applicant respectfully disagrees with the rejection. However, to expedite prosecution, Applicant has amended claims 37-43 to more clearly satisfy the claim statutory subject matter.

II. REJECTION UNDER 35 U.S.C. §102

The Office Action rejected claims 1-53 under 35 U.S.C. §102(e) as being anticipated by U.S. Publication No. 20050084112 by Kim et al. (hereinafter "Kim").

To anticipate a claim under 35 U.S.C. § 102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

Applicant respectfully submits that Kim fails to teach the claimed limitations.

Kim teaches an apparatus for generating scrambling codes in hardware. Figure 10 teaches a first m-sequence generator 1050 that generates a first m-sequence using first shift register memory 1040. A second m-sequence generator 1060 generates a second m-sequence using a second shift register memory 1045. The first and second m-sequence generators 1050 and 1060

generate respective serial output sequence bits according to each generation polynomials at every period of the input clock. The first m-sequence passes through masking sections 1000 to 1005 that store mask code values for generating cyclical shifts of the first m-sequence. Bits of the first m-sequence and the second m-sequence are added 1030 to generate a primary scrambling code. Bits of the cyclically shifted first m-sequence and the second m-sequence are added 1032 and 1034 to generate secondary scrambling codes.

In the present claimed invention, a linear shift register is used to generate a first array of values and a second array of values. Output values are generated from the first array and mask values are generated from the second array. The output values are then combined with the mask values to generate a key stream block.

Claims 1, 27, 37 and 44

As to independent claims 1, 27, 37 and 44, the Office Action alleges that Kim teaches "*applying a cryptographic function* on input values selected from a first array of values to generate output values" (emphasis added), "selecting mask values from a second array of values" and "combining the output values with the mask values to generate a key stream block for the key stream." Applicant submits that Kim does not teach applying a cryptographic function on the input values from the first array of values. In particular, the output values from registers 1050 and 1060 of Figure 10 do not pass through a cryptographic function as claimed. The first m-sequence (from register 1050) is passed directly to the masking sections 1000 to 10005 without being cryptographically altered. While Kim (Fig. 10) shows that a binary adder adds registers 0 to 7 and stores the sum into register 17, this is done as part of generating new bits in the first shift register 1050 and not to cryptographically modify input values to obtain output values as claimed. (See Paragraph [0065]).

Additionally, Kim does not teach "selecting mask values from a second array of values" as claimed. Kim teaches using a plurality of masking sections 1000 to 1005 in which each masking section has a different fixed mask value. (See Paragraph [0067]). Each value of the first m-sequence then passes (in parallel) through all the masking sections 1000 to 1005. In such configuration, no *selection* of "mask values from a second array of values" is performed since the mask sections have fixed mask values.

Moreover, Kim also fails to teach "combining the output values with the mask values to *generate a key stream block for the key stream.*" (Emphasis added). The system architecture taught by Kim is aimed at generating multiple scramble codes very quickly but not necessarily as securely as the key stream generated by the present claimed invention. In particular, Kim teaches combining the first m-sequence with different mask sections (each mask section having a single fixed mask value) to produce multiple scrambling codes or streams from each mask section. Thus, each scramble code is based on a single mask section (value). By contrast, the present claimed invention combines multiple output values with multiple mask values to create a single key stream block.

For at least the foregoing reasons, Kim fails to teach the limitations of claims 1, 27, 37 and 44.

Claims 2, 28, 38, and 45

As to dependent claims 2, 28, 38, and 45, the Office Action alleges that Kim teaches "generating the second array from the first array." Applicant submits that Kim fails to teach that the second array is generated from the first array. In particular, the system architecture disclosed by Kim uses fixed value mask sections 1000 to 1005 that are not generated based on the first m-sequence in register 1050. (See Paragraph [0067]). Additionally, the second m-sequence

(register 1060) is also not based on the first m-sequence (register1050). Consequently, Kim fails to teach this limitation as well.

Claims 3-5

As to dependent claims 3-5, the Office Action alleges that Kim teaches (Claim 4) "clocking the LFSR to generate the second array." As alleged in Office Action, the second array would correspond to the values stored in masking sections 1000 to 1005. Such values are fixed (see paragraph [0067]) and not generated based on clocking the linear feedback shift register (LFSR) used to generate the first array. Kim fails to teach that a single LFSR is used to generate both the first and second arrays.

Claims 6-8 and 29

As to dependent claims 6-8 and 29, the Office Action alleges that Kim teaches an "applying the cryptographic function on updated input values selected from an updated first array of values to generate updated output values", "selecting updated mask values from an updated second array of values" and "combining the updated output values with the updated mask values to generate a new key stream block for the key stream." These limitations are similar to those of independent claim 1. As previously explained with reference to claim 1, the system architecture taught by Kim is aimed at generating multiple scramble codes very quickly but not necessarily as securely as the key stream generated by the present claimed invention. First, Kim does not teach using a cryptographic function to generate the updated output values. In fact, no cryptographic function is applied to the updated input values by Kim. Secondly, Kim stores fixed masking values in masking sections 1000 to 1005. There is no updating or selection of such masking values as claimed. Thirdly, in Kim, multiple scramble codes are generated where each scramble

code is based on a single mask section (having a fixed mask value). By contrast, the present claimed invention combines multiple output values with multiple mask values to create a single key stream block. Consequently, Applicant submits that Kim fails to teach the claimed invention.

Claims 9, 30, and 46

As to dependent claims 9, 30, and 46, the Office Action alleges that Kim teaches "the number of input values and the number of output values are equal." Kim (Figure 10) teaches using a first and second m-sequence to generate multiple scramble codes. Thus, the number of output values of Kim is greater than the number of input values. Consequently, Applicant submits that Kim fails to teach the claimed limitation.

Claims 11, 31, and 48

As to dependent claims 11, 31, and 48, the Office Action alleges that Kim teaches "each value comprises of one or more words and wherein each word comprises two or more bytes." Applicant submits that Kim (Figure 10) teaches a scramble code generator based on bit streams and bit-wise operations. (See Paragraph [0063]). The system described by Kim in Figure 10 appears to operate on bits and not words as claimed.

Claims 12-26, 32-36, 39-43, and 49-53

As to claims 12-26, 32-36, 39-43, and 49-53, the Office Action alleges that Kim teaches the recited limitations. However, Applicant submits that Kim fails to teach these limitations.

As to claims 12, 32, 39, and 49, Kim does not teach or suggest "performing a byte-wise substitution of at least one byte of an input value to generate primary intermediate values" as claimed. No byte-wise substitution as claimed is taught by Kim.

As to claims 14, 40, and 50, Kim fails to teach "perform a key-dependent Sbox substitution on the at least one byte." As previously discussed, Kim (Figure 10) teaches bit-wise operations not byte-wise operations and no key-dependent substitution box is used.

As to claim 16, Kim does not teach or suggest "generating the first key byte based on a secret key of one or more words." Kim does not appear to teach the use of a secret key as claimed.

As to claim 17, Kim does not teach or suggest "performing a byte-wise substitution of at least one byte of a word of the secret key to generate a corresponding replacement word." Kim fails to teach byte-wise substitution as claimed.

As to claim 18, Kim does not teach or suggest "combining a second key byte with the substituted first combined byte to generate a second combined byte." Kim fails to teach the use of key bytes as claimed.

As to claims 19, 34, 41 and 51, Kim does not teach or suggest "mixing at least two bytes using a minimum distance separable matrix multiplication." Kim fails to teach using a minimum distance separable matrix multiplication as claimed.

As to claim 20, Kim does not teach or suggest "minimum distance separable matrix multiplication comprises operations over a Galois Field comprising 256 elements." Kim fails to teach operations over a Galois Field as claimed.

Kim similarly fails to teach the limitations recited in the remaining claims.

For at least the foregoing reasons, Applicant respectfully requests a withdrawal of the rejection under 35 U.S.C. §102.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

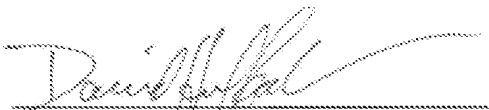
CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests a three-month extension of time in which to respond to the Office Action dated November 1, 2006. Please charge the requisite extension fee to Deposit Account No. 17-0026. Please charge any other fees associated with this paper to deposit Account No. 17-0026.

Respectfully submitted,

Dated: May 1, 2007

By: 
David J. Huffaker, Reg. No. 56,771
Attorney for Applicant
Telephone: 858-845-2110

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502